

CONSUMER FIRST

10th Edition

Child as Consumer Online

Old Enough — Age, Consent and the Marketplace

Governments are drawing age lines around the internet. But verifying a child's age is only the beginning.

FIVE FIGURES THAT DEFINE THIS EDITION

13	15	16	13-17	₹5 lakh
laws in California's new child online-safety package	minimum social-media age Macron wants across the EU	age threshold in Canada's proposed Safe Social Media Act (Bill C-34)	age band for OpenAI's new ChatGPT for Teens	CCPA penalty over non-compliant toy listings

BEYOND THE AGE GATE: How old is old enough for the internet?

How the EU's KIDS Act Could Reshape Age Assurance.

The EU's proposed KIDS Act would introduce a three-tier age framework for social media and video-sharing platforms: children under 13 would generally be unable to create their own accounts, users aged 13–14 would require supervised “mini accounts,” and those aged 15–17 could access services independently while retaining additional safety-by-design protections. The proposal also sets out when platforms must use age verification or other forms of age assurance, while building on existing obligations under the Digital Services Act.

Read Further: [Tech Policy Press](#).

Macron Pushes for EU-Wide Social Media Restrictions for Under-15s

French President Emmanuel Macron has called for an EU-wide restriction on social media access for children under 15, framing the proposal as part of a broader effort to strengthen online protections for minors. The push adds to ongoing European debates around age verification, platform responsibility, and whether minimum-age rules should be harmonized across member states.

Read Further: [Source Link](#)



Canada Tests a “Safe Social Media” Alternative to a Teen Ban

Canada’s proposed **Safe Social Media Act (Bill C-34)** would introduce an under-16 social media limit, but unlike a straightforward prohibition, platforms could receive exemptions if they demonstrate that their services meet a high safety standard for children. The bill would also create a dedicated Digital Safety Commission with audit, enforcement and rule-making powers, while requiring platforms to address harmful content, addictive design features, child sexual abuse material, synthetic content and risks associated with AI companion chatbots. Age-assurance measures would include privacy safeguards, including limits on how age-verification data can be used and retained. The proposal therefore shifts part of the regulatory focus from simply restricting young users’ access toward requiring platforms to demonstrate that their products are sufficiently safe for them.

Read Further: [Source Link](#)



PROVE YOUR AGE — WITHOUT PROVING WHO YOU ARE.

Discord Reworks Age Assurance After Privacy Backlash

Discord has begun rolling out a revised age-assurance system that relies primarily on account-level signals rather than requiring every user to submit an ID or facial scan. The platform says it can estimate whether an account likely belongs to a teenager or an adult using factors such as account tenure, activity patterns, connected games and communities, while excluding message content and private conversations from the assessment. Discord expects more than 90% of users to be classified without an additional verification step.

The approach follows significant user backlash to an earlier verification model that relied more heavily on selfies and government IDs, with privacy concerns amplified by a 2025 breach involving a third-party provider that exposed identification data belonging to around 70,000 users. Users whose age cannot be confidently estimated, or who believe they have been incorrectly classified, may still be asked to use options such as a payment method, app-store information, an age credential, selfie-based estimation or identification documents. The rollout highlights a central challenge for age assurance: establishing whether someone is old enough to access a service while minimising the amount of identity data collected in the process.

Read Further: [Source Link](#)

REPORTING AND ACCOUNTABILITY

Meta Agrees to Share Child-Safety Reports with the Indian Government

Meta has agreed to report cases involving child sexual abuse material and other child-safety concerns to India's Ministry of Electronics and Information Technology, following discussions with the government on platform accountability and online safety. The move is aimed at improving coordination between the company and Indian authorities when serious child-safety risks are identified on Meta's platforms.

The development also reflects a broader regulatory push in India to make large digital platforms more responsive to harmful content involving minors, while raising questions around reporting standards, inter-agency coordination, and how platforms balance safety obligations with user privacy and due process.

Read Further: [Source Link](#)

When the Algorithm Stops Looking Like a Mere Middleman

The National Human Rights Commission (NHRC) has asked MeitY and the Ministry of Information and Broadcasting to examine whether Meta's increasingly active use of AI and algorithmic systems could alter its legal status as an intermediary. The notice follows allegations that paid Instagram advertisements promoted or facilitated access to child sexual abuse material, and asks regulators to consider Meta's role not just in hosting content, but in generating, modifying, curating, recommending, amplifying and monetizing it.

Read Further: [Source Link](#)



THE CHILD-SAFE PRODUCT



Beyond Age Gates: Why Child Safety Rules Must Also Regulate Platform Design

This ORF analysis argues that child online safety cannot be addressed through age-gating alone. As internet access expands rapidly in India, the more important policy question is no longer just how to keep children off certain services, but how platforms are designed once children are already online. The piece places the focus on the architecture of digital services — including recommendation systems, engagement features, and exposure pathways — rather than treating age verification as a complete solution.

The article also suggests that regulation should focus on measurable child-safety outcomes, especially how frequently children encounter harmful or age-inappropriate content, rather than relying only on whether a platform has age thresholds on paper. In that sense, the piece pushes policymakers to move from a narrow “who gets in” model to a wider “what happens inside” model of online safety. That makes platform design itself — not just user age — a core subject of regulation.

Five questions this edition lays for Indian policymakers

1. Should India pursue an outright age restriction, or differentiated age-based accounts?
2. How can age be assured without excessive collection of biometric or identity data?
3. Should addictive-design features be restricted directly for minors?
4. Should platforms have to demonstrate that a service is safe before serving minors?
5. How should responsibility be divided among platform, AI, privacy and consumer-protection regulators?

Link to the ORF Report: [Read More](#)

THE ONLINE CHILD IS A CONSUMER TOO

If Toys Need Safety Standards, What About Algorithms?

India's consumer regulator has fined an e-commerce platform Rs 5 lakh for allowing the sale of toys that failed mandatory BIS standards, holding that platforms cannot avoid responsibility simply by describing themselves as intermediaries. The CCPA said that a technologically advanced marketplace should have tools to detect and prevent the listing of regulated or prohibited products, especially where non-compliance creates safety risks for children.

The case offers a useful analogy for digital child safety. If physical products for children are expected to meet a chain of standards — testing, labelling, marketplace compliance, and enforcement — the obvious policy question is what equivalent framework should apply to digital systems that shape children's experiences online. As regulators increasingly scrutinise recommendation systems, feeds, and AI-driven services, the issue is no longer only whether harmful products are sold, but what safety obligations should attach to the design and operation of child-facing digital environments.

Read More: [Link](#)



OpenAI Builds a Teen-Specific Safety Layer into ChatGPT

OpenAI is introducing a dedicated ChatGPT experience for users aged 13–17, with stricter safeguards around self-harm, eating disorders, violence, sexual content, romantic roleplay, and emotional dependency. The system will also use age-prediction signals to place suspected minors into the teen experience by default, alongside parental controls and limited safety notifications. The shift reflects a broader move toward age-aware AI design, where safety features are built into the product experience rather than added only after harmful interactions occur.

Read More: [Source Link](#)



California Turns Child Online Safety Into a Design Obligation

California has enacted new child-safety rules targeting both social-media platforms and AI services, expanding the regulatory focus beyond age restrictions alone. The measures place greater emphasis on how digital products are designed for younger users, including safeguards around engagement features, harmful interactions, and AI systems that children may use directly. The development reflects a broader policy shift toward treating child safety as a product-design responsibility, rather than relying only on parental controls, content takedowns, or age gates.



Read More: [Source Link](#)